23/3/2008

تلميحات للأمان عند استخدام كمبيوتر عمومى

أعداد
طالب الطالب

talibaltalib@yahoo.com 009647808243318 Iraq | مهندس معماري

بسم الله الرحمن الرحيم

تلميحات للأمان عند استخدام كمبيوتر عمومي



هل تعدّ أجهزة الكمبيوتر آمنة في المكتبات ومقاهي إنترنت والمطارات؟

يعتمد ذلك على كيفية استخدامها! إليك هذه التلميحات التي ستساعدك على المحافظة على خصوصية معلوماتك الشخصية أو المالية.

1- لا تحفظ معلومات تسجيل الدخول. قم دائماً بتسجيل الخروج من المواقع على ويب عبر النقر فوق "تسجيل الخروج" على الموقع. فلا يكفي إغلاق إطار المستعرض ببساطة أو كتابة عنوان آخر.

تشمل برامج عديدة (وخاصة برامج الرسائل الفورية) ميزات تسجيل دخول تلقائي تحفظ اسم المستخدم وكلمة المرور. عطّل هذا الخيار لئلا يقوم شخصاً آخر بتسجيل الدخول باسمك.

2- لا تترك الكمبيوتر من دون مراقبة أثناء عرض معلومات حساسة على الشاشة. إذا اضطررت لترك الكمبيوتر العمومي، فقم بتسجيل الخروج من كافة البرامج وأغلق كافة الإطارات التي قد تعرض معلومات حساسة.

3- قم بمحو آثارك. تحتفظ مستعرضات ويب، مثل Internet Explorer، بسجل عن كلمات المرور وعن كل صفحة تزورها، وذلك حتى بعد أن تكون قد أغلقتها وسجلت الخروج منها.

لتعطيل الميزة التي تخزّن كلمات المرور

قبل الانتقال إلى ويب، أوقف تشغيل ميزة Internet Explorer التي "تتذكر" كلمات المرور.

1. انقر في Internet Explorer فوق أدوات، ثم انقر فوق خيارات إنترنت.

2. انقر فوق تبويب محتويات ثم انقر فوق إكمال تلقائي.

3. انقر لمسح علامتي تحديد خانات الاختيار المتعلقة بكلمات المرور.

لحذف ملفات إنترنت المؤقتة والمحفوظات الخاصة بك

عندما تنتهي من استخدام كمبيوتر عمومي، عليك حذف كافة الملفات المؤقتة ومحفوظات المواقع على إنترنت.

1. انقر في Internet Explorer فوق أدوات، ثم انقر فوق خيارات إنترنت.

2. في التبويب عام وضمن ملفات إنترنت المؤقتة، انقر فوق حذف الملفات، ثم فوق ملفات تعريف الارتباط.

3. ضمن محفوظات، انقر فوق مسح المحفوظات.

لحذف ملفات أخرى تم حفظها من قبل بوابات الشركة، على غرار Server Sharepoint Portal
في حال كنت تستخدم موقع لشركة على ويب يسمح لك بعرض مستندات داخلية للشركة، قد تكون تخزّن عن غير قصد مستندات حساسة في كمبيوتر عمومي.

1. احذف كافة الملفات الموجودة في المجلد المؤقت لحساب المستخدم الخاص بك، والذي يمكن البحث عنه باستعراض

.C:\Documents and Settings\username\Local Settings\Temp

2. في حال كانت شركتك تستخدم Microsoft Office SharePoint Portal Server، قم بإفراغ المجلد المؤقت (المستندات/مسودات SharePoint).

4- تنبّه للمتطفلين الذين يسترقون النظر. عندما تستخدم كمبيوتر عمومي، ابق متيقظاً للّصوص الذين يسترقون النظر عندما تُدخل كلمات مرور حساسة، وذلك لجمع المعلومات الخاصة بك.

5- لا تُدخل معلومات حساسة في كمبيوتر عمومي. توفر هذه الإجراءات بعض الحماية ضد المتطفلين العرضيين الذين يستخدمون الكمبيوتر العمومي بعد أن تكون قد استخدمته بنفسك.

ولكن لا تنسى أنه من المحتمل أن يكون لصوص مجتهدون قد ثبّتوا على الكمبيوتر العمومي برامج متقدمة تسجّل كل ضغط للمفاتيح، ثم ترسل هذه المعلومات بواسطة البريد الإلكتروني إلى اللصوص المذكورين.

وعندها، لا يهم إذا لم تحفظ المعلومات أو إذا محوت آثارك. فيبقى بإمكان هؤلاء الأشخاص الوصول إلى المعلومات.

إذا أردت فعلاً أن تكون بأمان، تجنّب كتابة رقم بطاقة الاعتماد أو أية معلومات مالية أو معلومات حساسة على أي كمبيوتر عمومي.

المصدر : موقع مايكروسوفت العربية

بالنسبة للنقطة الأخيرة فينصح بفتح برنامج المفكرة واستخدامه كمضلل أثناء كتابة كلمات السر والمعلومات المهمة ، وذلك بكتابة كلمات غير مفهومة وحروف بين كلمات السر فيه والتنقل بينه وبين خانة كلمات السر .





بكالوريوس هندسة معمارية بتقدير جيد من جامعة بغداد

talibaltalib@yahoo.com

talibaltalib2008@gmail.com

tel:

009647808243318